Solaris (Trademark of Sun Microsystems) operating system, the following conditions must be checked: (1) the scanned server is running the Solaris operating system, and (2) the scanned server is running LPD. Thus, the rules are constructed to define a vulnerability if these two conditions are present.

IN THE CLAIMS:

Cancel claims 1-4 and add new claims 5-40 as follows:

5. A system for protecting a network, comprising:

a vulnerability detection system (VDS) for gathering information about the network to determine vulnerabilities of a host on the network; and

an intrusion detection system (IDS) for examining network traffic responsive to the vulnerabilities determined by the VDS to detect traffic indicative of malicious activity.

6. The system of claim 5, wherein the VDS is adapted to gather information about the network by sending data to the host and receiving responsive data from the host.

7. The system of claim 5, wherein the VDS is adapted to gather information automatically provided by the host.

8. The system of claim 5, further comprising:

a vulnerabilities rules database, in communication with the VDS, for storing rules describing vulnerabilities of the host,

wherein the VDS is adapted to analyze the gathered information with the rules to determine the vulnerabilities of the host.

9. The system of claim 8, wherein the VDS is adapted to analyze the gathered information with the rules to identify an operating system on the host and determine the vulnerabilities responsive to the operating system.

10. The system of claim 8, wherein the VDS is adapted to analyze the gathered information with the rules to identify an open port on the host and determine the vulnerabilities based on the open port.

11. The system of claim 8, wherein the VDS is adapted to analyze the gathered information with the rules to identify an application executing on the host and determine the vulnerabilities based on the application.

12. The system of claim 5, further comprising:

an intrusion rules database, in communication with the IDS, for storing rules describing malicious activity,

wherein the IDS is adapted to analyze the network traffic with the rules to detect network traffic indicative of exploitations of the determined vulnerabilities.

13. The system of claim 5, wherein the IDS is adapted to detect traffic indicative of exploitations of only the determined vulnerabilities.

14. The system of claim 5, wherein the VDS is adapted to verify the determined vulnerabilities, and the IDS is adapted to detect traffic indicative of exploitations of only the verified vulnerabilities.

15. The system of claim 5, wherein the VDS is adapted to update the determined vulnerabilities, and wherein the IDS is adapted to detect traffic indicative of malicious activity in response to the update.

16. The system of claim 15, wherein the VDS is adapted to update the determined vulnerabilities in response to a change in the network.

17. A method for protecting a network, comprising:

gathering information about the network to determine vulnerabilities of a host on the network; and

examining network traffic responsive to the determined vulnerabilities to detect network traffic indicative of malicious activity.

18. The method of claim 17, wherein gathering information comprises sending data to a host on the network and receiving responsive data from the host.

19. The method of claim 17, wherein gathering information comprises receiving data automatically provided by the host on the network.

20. The method of claim 17, further comprising:

storing rules to describe vulnerabilities of the host,

wherein determining vulnerabilities includes analyzing the gathered information with the rules.

21. The method of claim 20, wherein determining vulnerabilities comprises analyzing the gathered information with the rules to identify an operating system on the host.

22. The method of claim 20, wherein determining vulnerabilities comprises analyzing the gathered information with the rules to identify an open port on the host.

23. The method of claim 20, wherein determining vulnerabilities comprises comparing the gathered information against the rules to identify an application on the host.

24. The method of claim 17, further comprising:

storing rules describing malicious activity,

wherein detecting network traffic indicative of malicious activity comprises analyzing the network traffic with the rules to detect traffic indicative of exploitations of the determined vulnerabilities.

25. The method of claim 17, wherein examining network traffic consists of detecting traffic indicative of exploitations of only the determined vulnerabilities.

26. The method of claim 17, further comprising:

verifying determined vulnerabilities,

wherein examining network traffic consists of detecting traffic indicative of the exploitations of only the verified vulnerabilities.

27. The method of claim 17, further comprising:

updating the determined vulnerabilities in response to a change in the network; and detecting traffic indicative of malicious activity in response to the update.

28. The method of claim 27, wherein the updating is responsive to a change in the network.

29. A computer program product, comprising:

a computer-readable medium having computer program logic embodied therein for protecting a network, the computer program logic:

gathering information about the network to determine vulnerabilities of a host on the network; and

examining network traffic responsive to the determined vulnerabilities to detect network traffic indicative of malicious activity.

A

30. The computer program product of claim 29, wherein gathering information comprises sending data to a host on the network and receiving responsive data from the host.

31. The computer program product of claim 29, wherein gathering information comprises receiving data automatically provided by the host on the network.

32. The computer program product of claim 29, further comprising:
storing rules to describe vulnerabilities of the host,
wherein determining vulnerabilities includes analyzing the gathered information with the rules.

33. The computer program product of claim 32, wherein determining vulnerabilities comprises analyzing the gathered information with the rules to identify an operating system on the host.

34. The computer program product of claim 32, wherein determining vulnerabilities comprises analyzing the gathered information with the rules to identify an open port on the host.

35. The computer program product of claim 32, wherein determining vulnerabilities comprises comparing the gathered information against the rules to detect an application on the host.

36. The computer program product of claim 29, further comprising:
storing rules describing malicious activity,
wherein detecting network traffic indicative of malicious activity comprises analyzing the network traffic with the rules to detect traffic indicative of exploitations of the determined vulnerabilities.

37. The computer program product of claim 29, wherein examining network traffic consists of detecting traffic indicative of exploitations of only the verified vulnerabilities.

38. The computer program product of claim 29, further comprising:

verifying determined vulnerabilities,

wherein examining network traffic consists of detecting traffic indicative of the exploitations of only the verified vulnerabilities.

39. The computer program product of claim 29, further comprising:

updating the determined vulnerabilities in response to a change in the network; and

detecting traffic indicative of malicious activity in response to the update.

40. The computer program product of claim 29, wherein the updating is responsive to a change in the network.